PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G06F 1/00, G11B 20/00 — A1

(11) Numéro de publication internationale: WO 98/04966

(43) Date de publication internationale: 5 février 1998 (05.02.98)

(21) Numéro de la demande internationale: PCT/FR97/01362

(22) Date de dépôt international: 22 juillet 1997 (22.07.97)

(30) Données relatives à la priorité:
96/09443 26 juillet 1996 (26.07.96) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: THOMSON-CSF [FR/FR]; 173, boulevard Haussmann, F-75008 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: DEVAUX, François [FR/FR]; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR). HUOT, Jean-Claude [FR/FR]; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR).

(74) Mandataires: BEYLOT, Jacques etc.; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR).

(81) Etats désignés: CA, JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

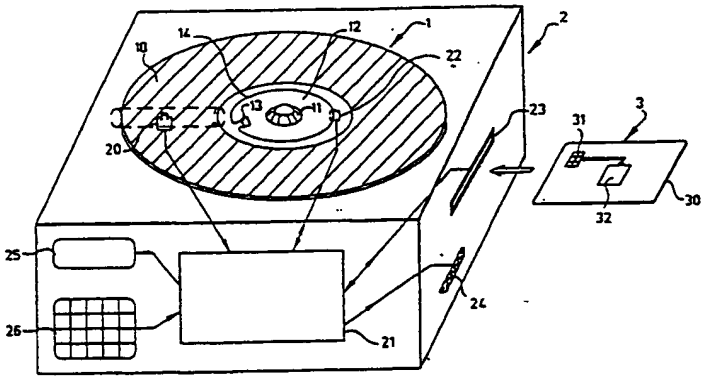
Publiée
Avec rapport de recherche internationale.

(54) Title: SYSTEM FOR SECURE DATA STORAGE ON CD-ROM

(54) Titre: SYSTEME DE STOCKAGE SECURISE DE DONNEES SUR CD-ROM

(57) Abstract

A system for effectively protecting confidential encrypted data stored on a CD-ROM by using a decryption key which is never accessible in unscrambled form to the user. In addition to the CD-ROM (1) on which the data at least partially encrypted by means of an encryption algorithm having a decryption key (K) is stored, and a CD-ROM player, the system comprises an electronic decryption microcircuit (13) embedded in said CD-ROM (1); means for data communication between the CD-ROM player (2) and the electronic decryption microcircuit (13) embedded in the CD-ROM (1); a smart card (3) containing at least one portion (K_1) of the decryption key (K), the optional remaining portion (K_2) of the decryption key (K) being included in the electronic decryption microcircuit (13) embedded in the CD-ROM (1); and means for secure data communication between the smart card (3) and the electronic microcircuit (13) embedded in the CD-ROM (1). For decryption, the encrypted data read out of the CD-ROM (1) is input into the electronic decryption microcircuit (13) embedded in the CD-ROM (1), which temporarily and transiently stores a decryption key received from the smart card (3) by secure transmission at the start of the read-out process, and uses it to decrypt the data before restoring the decrypted data for use.



(57) Abrégé

Ce système a pour but d'assurer une protection efficace de la confidentialité de données cryptées et stockées sur un CD-Rom par l'utilisation d'une clé de décryptage qui n'est jamais accessible en clair à l'utilisateur. Il comporte, outre le CD-Rom (1) sur lequel sont stockées des données cryptées au moins en partie avec un algorithme cryptographique ayant une clé de décryptage K et un lecteur de CD-Rom: un microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1); des moyens d'échange d'informations entre le lecteur de CD-Rom (2) et le microcircuit électronique de décryptage (13) enrobé dans le CD-Rom (1); une carte à puce (3) renfermant au moins une partie K_1 de la clé de décryptage K, la partie restante éventuelle K_2 de la clé de décryptage K figurant dans le microcircuit électronique de décryptage (13) enrobé dans le CD-Rom (1) et des moyens sécurisés d'échange d'informations entre la carte à puce (3) et le microcircuit électronique (13) enrobé dans le CD-Rom (1). Pour le décryptage, les données lues cryptées sur le CD-Rom (1) sont envoyées au circuit électronique de décryptage (13) enrobé dans le CD-Rom (1) qui stocke, de façon provisoire et fugitive, une clé de décryptage reçue de la carte à puce (3), par une transmission sécurisée, en début de session de lecture, et l'utilise pour le décryptage des données avant de retourner les données décryptées en vue de leur exploitation.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

SYSTEME DE STOCKAGE SECURISE DE DONNEES SUR CD-ROM

La présente invention concerne la protection de la confidentialité de données stockées sur un CD-Rom.

La seule possibilité pour sauvegarder la confidentialité de données stockées sur un CD-Rom est le cryptage. Cependant, cette protection n'est réellement satisfaisante que dans la mesure où la clé de décryptage reste inaccessible de l'utilisateur, ce qui n'est pas le cas lorsque la clé de décryptage est stockée sur le CD-Rom ou fournie à l'utilisateur par un autre biais. De plus il existe souvent un risque important de piratage de la clé de décryptage au niveau du circuit électronique de décryptage lui-même, qu'il soit situé dans le lecteur de CD-Rom ou en aval.

Diverses tentatives ont déjà été faites pour résoudre ce problème.

Dans le cas des cassettes ou des disquettes magnétiques qui sont enfermées dans un boîtier inamovible, il est connu, par la demande de brevet internationale WO-A-89/12890, d'équiper le boîtier d'une puce électronique pourvue de contacts électriques. Les données sont codées sur le support d'enregistrement, que ce soit une cassette ou une disquette magnétique, et décodées par l'intermédiaire de la puce électronique équipant le boîtier. Ce genre de protection n'est pas utilisable avec un CD-Rom car celui-ci n'est pas présenté dans un boîtier inamovible. En outre, il n'est pas parfaitement sûr car la clé de décodage doit être connue d'un utilisateur autorisé qui peut en faire profiter à loisir d'autres utilisateurs même non autorisés possédant le lecteur adéquat.

Dans le cas de CD-Rom, il est connu par la demande de brevet allemand DE-A-43 07 395, de coder les données enregistrées sur le CD-Rom à l'aide d'une clé ou mot de passe et de stocker le mot de passe dans une carte à puce. Cela permet, a priori, d'éviter l'utilisation des données du CD-Rom par des utilisateurs n'étant pas en possession de la carte à puce. Il subsiste cependant un risque de piratage par le fait que le mot de passe n'est pas réellement en sécurité à l'intérieur du lecteur de CD-Rom ou du CD-Rom lui-même.

La présente invention a pour but de remédier à ces divers inconvénients et d'assurer une protection efficace de la confidentialité de données stockées sur un CD-Rom.

Elle a pour objet un système de stockage sécurisé de données sur CD-Rom comportant un CD-Rom sur lequel sont stockées des données cryptées au moins en partie avec un algorithme cryptographique ayant une clé de décryptage K et un lecteur de CD-Rom. Ce système de stockage sécurisé de données est remarquable en ce qu'il comporte en outre :

- un microcircuit électronique de décryptage enrobé dans ledit CD-Rom,
- des moyens d'échange d'informations entre le lecteur de CD-Rom et le microcircuit électronique de décryptage enrobé dans le CD-Rom,
- une carte à puce renfermant au moins une partie K_1 de la clé de décryptage K, la partie restante éventuelle K_2 de la clé de décryptage K figurant dans le microcircuit électronique de décryptage enrobé dans le CD-Rom et
- des moyens sécurisés d'échange d'informations entre la carte à puce et le microcircuit électronique enrobé dans le CD-Rom.

Grâce à ce système, la confidentialité des données stockées sur CD-Rom est assurée au moyen d'un cryptage dont la clé de décryptage n'est jamais accessible en clair à l'utilisateur ce qui réduit dans une large mesure les risques de fraude.

Le microcircuit électronique de décryptage enrobé dans le CD-Rom est avantageusement pourvu d'une antenne inductive ou capacitive permettant d'assurer depuis l'extérieur du CD-Rom, en l'absence de tout contact, à la fois son alimentation électrique et des échanges d'informations.

Le lecteur de CD-Rom est avantageusement pourvu d'un connecteur de carte à puce et d'un circuit électronique assurant, outre la lecture du CD-Rom, la gestion des liaisons d'échange d'informations entre lui-même, le microcircuit électronique enrobé dans le CD-Rom et la carte à puce.

La carte à puce est avantageusement pourvue d'un code d'identification de son propriétaire qui doit obligatoirement lui parvenir en début de session pour qu'elle accepte de communiquer avec l'extérieur, tandis que le lecteur de CD-Rom est équipé de moyens de surveillance de la présence ininterrompue d'une carte à puce dans son connecteur de carte à puce tout au long d'un décryptage effectué par le microcircuit électronique enrobé dans le CD-Rom.

D'autres caractéristiques et avantages de l'invention ressortiront de la description ci-après d'un mode de réalisation de l'invention donné à titre d'exemple. Cette description sera faite en regard du dessin dans lequel la figure unique illustre, de manière schématique, l'architecture du système de stockage sécurisé de données sur CD-Rom selon l'invention.

On distingue sur cette figure un CD-Rom 1 posé sur un lecteur de CD-Rom 2 équipé d'un connecteur de carte à puce 23 dans lequel vient s'insérer une carte à puce 3.

Le CD-Rom 1 présente, comme tout CD-Rom classique, une plage annulaire gravée 10 où sont stockées les données, un trou de centrage 11 et, autour de ce trou de centrage 11, une plage centrale 12 permettant sa préhension et son entraînement en rotation par le mécanisme d'un lecteur de CD-Rom. Il se différencie des CD-Rom classiques par le fait que les données qu'il stocke sont cryptées par un algorithme à clé K et donc non directement exploitables, et qu'il présente un microcircuit électronique de décryptage 13 avec une antenne inductive 14 enrobés dans le plastique de sa plage centrale 12. Le microcircuit électronique 13 de décryptage et son antenne inductive 14 relèvent, par leur conception, de la technique des cartes à puce sans contact. L'antenne 14, qui pourrait également être capacitive, permet à la fois l'alimentation électrique du microcircuit électronique de décryptage 13 et des échanges d'informations avec ce microcircuit électronique de décryptage 13 depuis l'extérieur du CD-Rom. Le microcircuit électronique de décryptage 13 comporte un microcontrôleur pourvu d'un port série d'entrée-sortie raccordé à l'antenne 14 et de mémoires vive de type RAM et morte de type ROM et éventuellement EEPROM. Il est programmé pour réclamer la clef de décryptage K ou la

partie qui lui manque K_1 de cette clé dés sa mise sous tension, la recevoir sous une forme sécurisée, la mettre en mémoire RAM, recevoir les données cryptées, les décrypter avec la clef de cryptage K obtenue stockée en mémoire RAM et retourner les données décryptées pour qu'elles soient exploitées. Il ne sera pas décrit en détail car il relève de la pratique habituelle pour un technicien du cryptage et du décryptage de données.

Le lecteur de CD-Rom 2 comporte les éléments habituels d'un lecteur de CD-Rom, dont le moteur d'entraînement en rotation du CD-Rom lu, la tête optique de lecture 20 à diode Laser et photodétecteur montée sur un équipage mobile se déplaçant selon un rayon du CD-Rom lu et un circuit électronique 21 assurant la gestion des déplacements de l'équipage mobile de sa tête de lecture 20 et une mise en forme des signaux issus de cette tête de lecture. En plus de ces éléments, il est pourvu d'un capteur 22 coopérant avec l'antenne 14 du circuit électronique de décryptage 13 enrobé dans le CD-Rom 1, du connecteur de carte à puce 23, d'un connecteur de communication extérieure 24, d'un afficheur 25 et d'un clavier 26. Son circuit électronique 21 assure, en plus des tâches habituelles de lecture d'un CD-Rom :

- la gestion du capteur 22 coopérant avec l'antenne 14 du circuit électronique de décryptage 13 enrobé dans le CD-Rom 1 pour assurer l'alimentation et les échanges d'informations avec ce dernier circuit de décryptage 13,
- la gestion du connecteur 23 de carte à puce de manière à assurer l'alimentation d'une carte à puce raccordée 3 et les échanges d'informations avec cette dernière,
- la gestion du connecteur de communication extérieure 24 afin de délivrer, à un système de traitement déporté, des données exploitables lues sur le CD-Rom 1 et décryptées par le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1, avec l'aide d'une clé de décryptage fournie par la carte à puce 3,
- la gestion de l'afficheur 25, et
- la gestion du clavier 26.

La carte à puce 3 comporte une carte support plastifiée 30 pourvue d'un ensemble de contacts 31 raccordés à un microcircuit

électronique 32 qui est représenté, par facilité, au milieu de la carte mais qui est en réalité enterré sous les contacts 31. Le microcircuit 32 renferme principalement, un microcontrôleur (CPU) en liaison avec un port série d'entrée-sortie (SIO) raccordé aux contacts 31 et avec de la mémoire en partie vive (RAM) et en partie permanente, à la fois de type morte non réinscriptible (ROM) et de type morte réinscriptible (EEPROM) destinée au stockage d'une partie au moins K_1 de la clé de décryptage et d'un programme gérant le protocole de communication sous une forme sécurisée de la partie K_1 de clé de cryptage résidant dans la carte à puce 3.

Au démarrage d'une lecture de données cryptées sur le CD-Rom 1, le lecteur de CD-Rom 2 alimente le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 qui demande alors la clé de cryptage K ou sa partie manquante K_1. En réponse, le lecteur de CD-Rom 2 met le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 en communication avec la carte à puce 3. Cette dernière réclame un code d'identification de la part de l'opérateur avant d'accepter le dialogue. Si sa réclamation est satisfaite positivement par l'opérateur qui tape au clavier 26 son code d'identification, la carte à puce 3 défère à la demande du microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 et lui communique, sous forme sécurisée, la clé de cryptage K ou sa partie manquante K_1. Le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 place alors la clé de cryptage complète K dans sa mémoire vive et informe le lecteur de CD-Rom 2 qu'il est près au décryptage. Le lecteur de CD-Rom 2 établit alors une communication ascendante et descendante avec le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1. Au cours de cette communication le lecteur de CD-Rom 2 fait parvenir au microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 les données cryptées qu'il lit dans le CD-Rom 1. Le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 décrypte les données reçues à l'aide de la clé de décryptage K présente dans sa mémoire vive et les retourne en clair au lecteur de CD-Rom 2 qui les dirige sur son connecteur de communication extérieure 24 pour qu'elles soient exploitées. Simultanément avec l'établissement de toute liaison de

communication avec le lecteur de CD-Rom 2, le circuit de décryptage 13 enrobé dans le CD-Rom 1 teste la présence effective de la carte à puce 3 dans son connecteur 23 et interrompt son fonctionnement en cas de retrait de la carte à puce, ce qui provoque la perte de la clé de décryptage K par le microcircuit de décryptage 13 enrobé dans le CD-Rom 1 et empêche de poursuivre un décryptage après retrait de la carte à puce.

La procédure d'authentification du porteur de la carte à puce préalable à tout dialogue avec cette dernière qui s'effectue par une demande de code secret ou "PIN CODE" à taper au clavier suivie d'une vérification de ce code secret est une procédure classique utilisée avec les cartes à puce employées pour des transactions et ne sera pas détaillée ici.

Le transfert sécurisé de tout ou partie de la clé de décryptage K dans la mémoire vive du microcircuit de décryptage 13 enrobé dans le CD-Rom 1 peut se faire selon le protocole suivant :

- Au cours d'une première étape, le microcircuit de décryptage 13 enrobé dans le CD-Rom 1 émet à l'intention de la carte à puce 3 une demande d'échange d'informations.

- Au cours d'une deuxième étape, la carte à puce 3, après un déroulement favorable de la procédure d'identification du porteur, répond par un signal d'acquiescement.

- Au cours d'une troisième étape, le microcircuit de décryptage 13 détecte le signal d'acquiescement de la carte à puce, engendre un aléa A (nombre binaire aléatoire) qu'il code avec une clé de cryptage-décryptage C_1 d'un algorithme cryptographique dissymétrique destiné à la sécurisation de la transmission et envoie à la carte à puce 3 sous forme d'un message crypté $C_1(A)$.

- Au cours d'une quatrième étape, la carte à puce 3 reçoit ce message crypté, le décrypte à l'aide d'une autre clé, en sa possession, de cryptage-décryptage C_2 de l'algorithme de cryptographique dissymétrique de transmission utilisé par le microcircuit de décryptage 13, et obtient l'aléa en clair :

$$C_2(C_1(A)) = A$$

- Au cours d'une cinquième étape, la carte à puce 3 réalise une opération logique de "ou exclusif" entre l'aléa A reçu du microcircuit de décryptage 13 et la clé de décryptage K des données du CD-Rom 1, ou une partie K_1 de cette clé manquant au microcircuit de décryptage et connue de la seule carte à puce 3. Pour simplifier, on suppose ici que la totalité de la clé K manque au microcircuit de décryptage 13 si bien que la carte à puce effectue l'opération :

$$A \oplus K = D$$

- Au cours d'une sixième étape, la carte à puce 3 code le résultat de cette opération logique avec la clé de cryptage-décryptage de transmission C_2 en sa possession et le transmet au microcircuit de décryptage 3 sous la forme :

$$C_2(D) = C_2(A \oplus K)$$

- Au cours d'une septième étape, le microcircuit de décryptage 13 reçoit ce message, le décrypte avec sa clé de cryptage-décryptage C_1 et obtient le message :

$$C_1(C_2(D)) = D$$

- Au cours d'une huitième et dernière étape, le microcircuit de décryptage 13 récupère la clé de décryptage K des données du CD-Rom 1 en soumettant le message reçu de la carte à puce 3 et décrypté à une opération logique de "ou exclusif" avec l'aléa A qu'il a engendré au départ :

$$D \oplus A = (A \oplus K) \oplus A = K$$

La procédure de transfert d'information de la carte à puce 3 en direction du microcircuit de décryptage 13 qui vient d'être décrite est sécurisée non seulement parce que les informations ne sont pas transférées en clair mais aussi parce que le cryptage de la transmission est partagé entre les deux intervenants et dépend d'un aléa qui change à chaque session.

Bien sûr, le protocole de communication sécurisée entre le microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 et la carte à puce 3 qui vient d'être décrit, n'est qu'un exemple et peut être remplacé par d'autres protocole utilisant des algorithmes de cryptage plus complexes comme le RSA, le DSA, etc...

Les échanges d'informations avec la carte à puce 3 se font, selon le protocole défini dans la norme ISO 7816/4, au moyen d'une commande "execute" lorsqu'il s'agit d'une transmission en direction de la carte à puce, et d'une commande "get challenge" lorsqu'il s'agit d'une transmission en provenance de la carte à puce.

Une manière de vérifier la présence de la carte à puce 3 dans le connecteur de carte à puce 23 du lecteur de carte à puce 2 tout au long d'une opération de lecture et décryptage des données du CD-Rom 1 consiste à engendrer périodiquement des aléas dans le microcircuit de décryptage 13, à les envoyer à la carte à puce 3 pour qu'elle les signe, c'est-à-dire qu'elle les crypte avec la clé de cryptage-décryptage C_2 de transmission en sa possession, puis les retourne, à décrypter les signatures de la carte à puce 3 avec la clé de cryptage-décryptage C_1 de transmission en possession du microcircuit électronique de décryptage 13 enrobé dans le CD-Rom 1 et à vérifier qu'elles correspondent bien à l'aléa envoyé. Comme aléas utilisés au cours de cette procédure de vérification de la présence de la carte à puce 3, le microcircuit de décryptage 13 enrobé dans le CD-Rom 1 pourra utiliser le résultat d'une opération logique de type "ou exclusif" entre les données cryptées et les données décryptées qu'il est en train de manipuler.

Avec le système de stockage sécurisé de données sur CD-Rom qui vient d'être décrit, la simple disponibilité du CD-Rom et de son lecteur spécialisé ne permet plus d'exploiter les données en dehors d'une attaque cryptographique classique dont la difficulté est fonction de l'algorithme de cryptage choisi. En effet, il manque la clé ou une partie de la clé de décryptage qui est stockée au sein de la carte à puce et qui n'est jamais accessible en clair pour l'utilisateur. Le fait de disposer en plus de la carte à puce n'est pas suffisant puisqu'il faut aussi connaître le code d'identification ou "PIN CODE" pour démarrer les opérations de décryptage, que celle-ci soit ou non restée dans le lecteur de CD-Rom au cours d'une précédente session.

On pourra prendre différentes précautions complémentaires, comme le changement régulier du code d'identification du porteur de la carte à puce ou "PIN CODE" ou la limitation du nombre de tentatives infructueuses d'utilisation de la carte à puce grâce à un processus

d'auto-inhibition de cette dernière. De plus, il peut être prévue une procédure d'initialisation lors d'une première lecture du CD-Rom, alors que celui-ci et sa carte à puce de clé de décryptage de données ne sont pas encore personnalisés. A la première lecture du CD-Rom, avec la carte à puce enfichée, la carte à puce demande à l'utilisateur de choisir un code d'identification qu'elle mémorise de manière définitive. Elle dialogue ensuite avec le microcircuit électronique enrobé dans le CD-Rom pour choisir les clés de cryptage-décryptage de leur liaison de transmission et se les répartir entre eux. A partir de ce moment, les secrets répartis entre le microcircuit électronique de décryptage enrobé dans le CD-Rom, la carte à puce de clé de décryptage de données et l'utilisateur rendent le fonctionnement du système impossible en l'absence de l'un de ses éléments et de la connaissance du code d'identification de l'utilisateur.

Le système qui vient d'être décrit est particulièrement intéressant, pour protéger des données sensibles concernant l'activité d'une entreprise, stockées sur un CD-Rom en vue de leur exploitation sur des ordinateurs personnels portables par un personnel habilité astreint à des déplacements fréquents.

Bien entendu, la présente invention n'est pas limitée à l'exemple décrit mais elle est susceptible de nombreuses variantes ressortant de la pratique courante de l'homme du métier.

REVENDICATIONS

1. Système de stockage sécurisé de données sur CD-Rom comportant un CD-Rom (1) sur lequel sont stockées des données cryptées au moins en partie avec un algorithme cryptographique ayant une clé de décryptage K et un lecteur de CD-Rom (2) caractérisé en ce qu'il comporte en outre :

- un microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1),
- des moyens d'échange d'informations entre ledit lecteur de CD-Rom (2) et ledit microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1),
- une carte à puce (3) renfermant au moins une partie K_1 de la clé de décryptage K, la partie restante éventuelle K_2 de la clé de décryptage K figurant dans ledit microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1) et
- des moyens sécurisés d'échange d'informations entre ladite carte à puce (3) et ledit microcircuit électronique (13) enrobé dans ledit CD-Rom (1).

2. Système selon la revendication 1, caractérisé en ce que ledit microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1) est pourvu d'une antenne (14) assurant, sans présence de contact, à la fois l'alimentation électrique dudit microcircuit de décryptage (13) depuis l'extérieur et les échanges d'informations avec l'extérieur.

3. Système selon la revendication 1, caractérisé en ce qu'il comporte en outre des moyens d'authentification d'un utilisateur autorisé de ladite carte à puce (3) imposant en préalable à un échange d'informations avec ladite carte à puce (3), la fourniture par l'utilisateur d'un code secret d'identification.

4. Système selon la revendication 1, caractérisé en ce qu'il comporte en outre des moyens de surveillance de la présence ininterrompue de ladite carte à puce (3) pendant le fonctionnement dudit

microcircuit électronique de décryptage (13) enrobé dans ledit CD-ROM (1).

5. Système selon la revendication 3, caractérisé en ce que ladite carte à puce (3) est pourvue de moyens d'inhibition limitant le nombre de tentatives infructueuses d'introduction du code secret d'identification.

6. Système selon la revendication 1, caractérisé en ce qu'il comporte des moyens d'initialisation permettant de personnaliser ladite carte à puce (3) et/ou les moyens sécurisés d'échange d'informations entre ladite carte à puce (3) et ledit microcircuit électronique de décryptage (13) enrobé dans ledit CD-Rom (1) en préalable à une première utilisation.

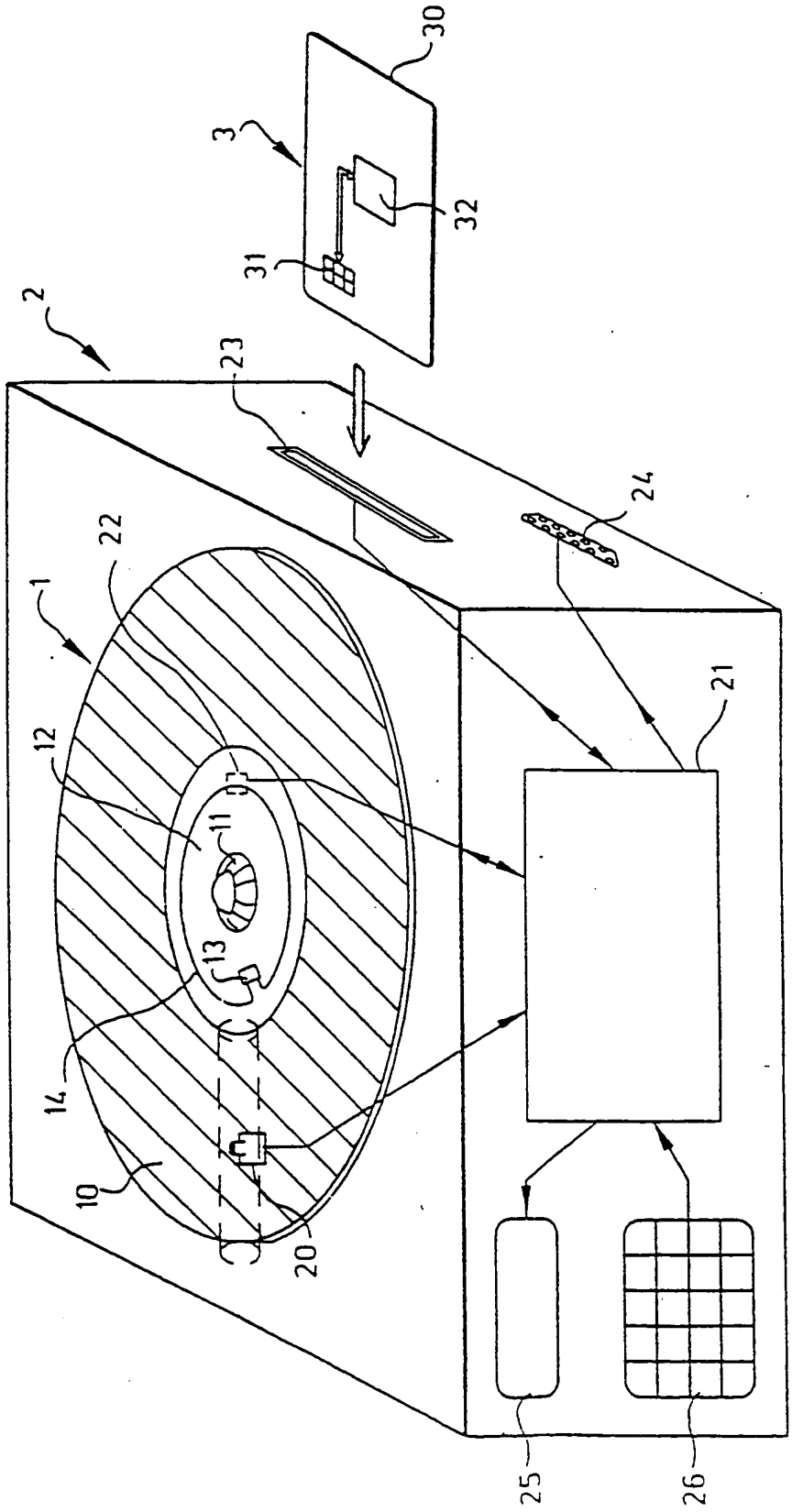


FIG.1

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/FR 97/01362

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 89 12890 A (DUPRE MICHEL JEAN) 28 December 1989 see abstract; claims 1-7,16	1
Y A	DE 43 07 395 A (BORUS SPEZIALVERFAHREN UND GER) 15 September 1994 see abstract; figure 1	1 3-6
A	FR 2 643 475 A (LIVOWSKY JEAN MICHEL) 24 August 1990 see abstract see page 14, line 7 - line 15; claims 1-13	1
P,X	WO 96 29699 A (MEILLER COMCARD GMBH ;LENDER FRIEDWART (DE); HORSTER PATRICK (DE)) 26 September 1996 see page 6, line 11 - page 9, line 3; figures 3,5	1-3

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 1997	13. 10. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/FR 97/01362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8912890 A	28-12-89	FR 2633086 A	22-12-89
DE 4307395 A	15-09-94	NONE	
FR 2643475 A	24-08-90	AU 5173790 A WO 9010292 A GR 90100111 A	26-09-90 07-09-90 28-06-91
WO 9629699 A	26-09-96	AU 5110596 A	08-10-96

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 97/01362

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G06F1/00 G11B20/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G06F G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 89 12890 A (DUPRE MICHEL JEAN) 28 décembre 1989 voir abrégé; revendications 1-7,16	1
Y	DE 43 07 395 A (BORUS SPEZIALVERFAHREN UND GER) 15 septembre 1994	1
A	voir abrégé; figure 1	3-6
A	FR 2 643 475 A (LIVOWSKY JEAN MICHEL) 24 août 1990 voir abrégé voir page 14, ligne 7 - ligne 15; revendications 1-13	1

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 septembre 1997	13.10.97

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

Demande internationale No
PCT/FR 97/01362

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
P,X	WO 96 29699 A (MEILLER COMCARD GMBH ;LENDER FRIEDWART (DE); HORSTER PATRICK (DE)) 26 septembre 1996 voir page 6, ligne 11 - page 9, ligne 3; figures 3,5 ---	1-3

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

(21) Int. Application Number: PCT/FR97/01362
(22) Int. Filing Date: 22 July 1997 (22.07.97)
(30) Priority Data: 96/09443 26 July 1996 (26.07.96) FR

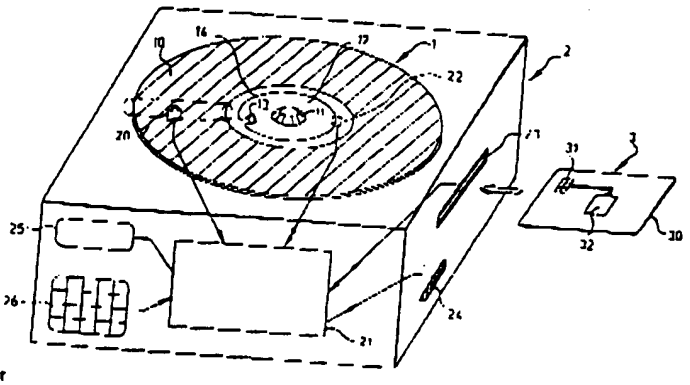
(71) Applicant (for all designated States except US): THOMSON-CSF [FR/FR]; 173, boulevard Haussmann, F-75008 Paris (FR).
(72) Inventors; and
(75) Inventors/Applicants (for US only): DEVAUX, François [FR/FR]; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR). HUOT, Jean-Claude [FR/FR]; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR).
(74) Agents: BEYLOT, Jacques et al.; Thomson-CSF S.C.P.I., 13, avenue du Président Salvador Allende, F-94117 Arcueil Cedex (FR).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(51) International Patent Classification 6: G06F 1/00, G11B 20/00
A1
(11) Int. Publication Number: WO 98/04966
(43) Int. Publication Date: 5 February 1998 (05.02.98)
G06F

(54) Title: SYSTEM FOR SECURE DATA STORAGE ON CD-ROM



(57) Abstract

A system for effectively protecting confidential encrypted data stored on a CD ROM by using a decryption key which is never accessible in unscrambled form to the user. In addition to the CD ROM (1) on which the data at least partially encrypted by means of an encryption algorithm having a decryption key (K) is stored, and a CD-ROM player, the system comprises an electronic decryption microcircuit (13) embedded in said CD-ROM (1); means for data communication between the CD-ROM player (2) and the electronic decryption microcircuit (13) embedded in the CD-ROM (1), a smart card (3) containing at least one portion (K_1) of the decryption key (K), the optional remaining portion (K_2) of the decryption key (K) being included in the electronic decryption microcircuit (13) embedded in the CD-ROM (1); and means for secure data communication between the smart card (3) and the electronic microcircuit (13) embedded in the CD ROM (1). For decryption, the encrypted data read out of the CD-ROM (1) is input into the electronic decryption microcircuit (13) embedded in the CD-ROM (1), which temporarily and transiently stores a decryption key received from the smart card (3) by secure transmission at the start of the read-out process, and uses it to decrypt the data before restoring the decrypted data for use.

(21) Int. Application Number: PCT/GB97/00241
(22) Int. Filing Date: 28 January 1997 (28.01.97)
(30) Priority Data: 9615597.3 25 July 1996 (25.07.96) GB

(71)(72) Applicants and Inventors: COLLINS, Peter, David [GB/GB]; 2 Spencers, Hawkwell, Hockley, Essex SS5 4LW (GB). ROYER, Karl, William [GB/GB]; 14 Buttermere Gardens, Aylesham, Kent CT3 3LT (GB). HOWYER, Mark, David, James [GB/GB]; 7 Southleigh Road, Havant, Hants PO9 2HR (GB).
(74) Agent: LEMING, John, Gerard; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5LX (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(51) International Patent Classification 6: C06F 1/00, G08B 25/01
A1
(11) Int. Publication Number: WO 98/04967
(43) Int. Publication Date: 5 February 1998 (05.02.98)

(54) Title: IMMOBILISATION PROTECTION SYSTEM FOR ELECTRONIC COMPONENTS

(57) Abstract

An electronic security system that embeds electronic immobilisation protection devices (IPDs) in electronic products and components. IPDs have controlled access to a security service provider (SSP). At power on, and periodically thereafter, the IPD sends a cryptographically secure "challenge" to the SSP. If a part has not been reported stolen, then the SSP replies with a valid cryptographically secure "response", otherwise it replies with an invalid "response". If the IPD receives an invalid "response", or when a limited time has elapsed without a "response", it renders the part inoperative. A valid "response", inside the time limit, allows the part to function normally. A stolen and recovered product can be identified and traced to its rightful owner, who contacts the SSP to re-enable the product. IPDs allow specific parts to function normally for a limited period of time, so that existing hardware, software and network resources can be utilised to communicate to the SSP.